

Gefahren im Internet!

Jeder sollte sich im Klaren darüber sein, dass der heimische Rechner jedes Mal beim Eintritt in die Datenautobahn (Internet) ein gefährliches Pflaster betritt.

Diese Autobahn fährt nämlich keineswegs nur in eine Richtung. Der Computer überträgt und erhält aus dem Internet ununterbrochen Daten. Es hat also absolut nichts mit Panikmache zu tun, wenn wir sagen, dass unter derzeit einer dreiviertel Milliarde Internetnutzer nicht nur Nette Leute unterwegs sind. Hacker und solche, die es werden wollen (Scriptkiddies) sowie Spammailversender oder Dialerbetreiber und, und, und lauern auch in der bunten weiten (Internet-) Welt. Und das sind nur einige....

Um allein mal festzuhalten, was alles so Möglich ist mal ein Beispiel:

- Frau Mustermann möchte für Ihre Kinder einige Fensterbild-Vorlagen (Windowcolor) runterladen um diese dann auszudrucken. Sie sucht bei einer Suchmaschine wie Google also nach "Windowcolor" und klickt auf einen der ersten 5 Ergebnistreiber. Nun wird Sie beim weiterklicken auf der Seite aufgefordert selber "OK" in das lustige kleine Formular einzugeben.

Was war passiert?

Sie hat nun einen **Dialer** auf dem heimischen Computer und durch Ihre Bestätigung mit "ok" hat sie mal eben etwa 30,- Euro ausgegeben. Dazu sei aber gesagt, dass heutzutage die User genau 3-mal selber OK eingeben müssen um eine teure Servicenummer anzuwählen.

Hacker versuchen anders und auch zum Teil mit anderen Hintergründen in ein System einzudringen. Bei nicht allen Angriffen steht die Geldbörse der User im Vordergrund. Viele Angriffe passieren tatsächlich, sagen wir mal aus sportlichem Ehrgeiz. Wie schwer mag es sein in dieses- oder jenes System einzudringen.

Mit Hilfe eines so genannten **IP-Scanners** (auch Portscanner genannt) werden ganze IP-Adressräume flächendeckend ausgespäht. Es wird dabei erstmals geprüft welche Netze überhaupt erreichbar sind. Wenn dann ein Netz, oder ein einzelner Rechner ausgemacht worden ist wird versucht über offene Ports in das Zielsystem einzudringen.

Mögliche Schäden durch Angriffe von Viren, Trojanern, Hackern, Spyware und was sonst noch auf ahnungslose Opfer lauert wären in etwa folgende:

- Harmlose aber störende Bildschirmanimationen
- Daten- bzw. Dateizerstörung durch Löschen oder Überschreiben
- Zerstörung von gesamten Disketten- bzw. Festplatteninhalten durch Formatieren
- Manipulation von Daten durch z.B.ersetzen bestimmter Zeichenketten
- Verfälschung der Tastatureingaben
- Beschädigung von Hardware durch z.B. die Erhöhung der Bildschirmfrequenz mittels der Grafikkarte hat manchmal ein Verschmoren der Leuchtschicht an der Bildschirminnenseite zur Folge.
- Bei manchen Diskettenlaufwerken verklemmt sich der Lese/Schreibkopf wenn versucht wird über die innerste Spur hinauszulesen.
- Die Überbeanspruchung eines elektronischen Bauteils wie z.B. des Co-Prozessors kann zu dessen Beschädigung führen.
- Blockierung von Speicherplatz durch z.B. das Schreiben riesiger Dateien mit sinnlosem Inhalt auf die Festplatte oder Diskette.
- das Laden sinnloser Programme in den Arbeitsspeicher.
- Reduzierung der Systemleistung durch z.B.: *) Verkleinerung des Arbeitsspeichers (siehe oben)
- Beanspruchung der Prozessorleistung für sinnlose Berechnungen.
- Blockierung von Programmen durch Aufforderung zur Eingabe eines Passwortes ohne dessen ein Programm nicht gestartet werden kann.
- Nichts

Wie hoch ist die potenzielle Gefahr eines Angriffs?

Nun, es kann sein, auch wenn es zu Anfang recht unwahrscheinlich ist, dass Sie sofort infiziert werden. Bei Hackern ist die Gefahr zu Anfang weit geringer. Interessant wird es meist erst, wenn Sie über einen Freemailer sich eine Email-Adresse einrichten. Sie werden dann schnell feststellen, dass Sie Unmengen an Mails bekommen von Leuten, die Sie gar nicht kennen.

Zumisst sind das Aufforderungen auf bestimmte Webseiten zu gehen um dort irgendwas zu kaufen. Die berühmten Penisvergrößerungen u.s.w.

Diese Emails nennt man gemeinhin Spammails.

Heutzutage ist leider schon Jeder Internetnutzer Ziel von Viren oder Hackerangriffen. Die meisten Viren beinhalten ein Spyprogramm, das versucht an geheime Daten auf Ihrem Rechner zu gelangen.

Interessant sind hier Daten, wie beispielsweise Kreditkartennummern oder Passwörter für Onlinebanking u.s.w.

Virenschutz, Antivirus

Doch wie hoch ist das Risiko denn nun wirklich? Kurz gesagt, umso länger Sie am Onlineleben teilnehmen, umso größer die Gefahr. Wenn Sie sich schon länger im Internet aufhalten, dann werden Sie gewiss auch an einigen Sachen Interesse haben wie z.B. Foren, Newsgroups, Chats, Online-Gaming u.s.w.

Sicher ist keine dieser Anwendungen doch sind Sie nicht allein im Web unterwegs. Der Schutz, den Sie also standartmässig haben ist wie...lassen Sie es mich so ausdrücken. Sie sind ein kleiner Fisch in einem großen Fischschwarm und verstecken sich im Schwarm.

Es empfiehlt sich daher wirklich sich ein gutesVirenschutzprogramm zuzulegen.

Viele Faktoren spielen eine Rolle, wie leicht/schwer Sie angreifbar sind. Um einige zu nennen:

- **verwendete Betriebssysteme (Windows ,Linux ,Apple...)**
- **verwendete Programme (Antivirussoftware)**
- **Welchen Browser (Internet Explorer IE ,Netscape, Firebird...)**
- **Internetverbindungsarten (Modem , ISDN ,DSL ..)**
- **Dauer einer Onlinesession erhöht auch die Angriffsgefahr, da der Computer länger unter einer IP erreichbar ist.**
- **Benutzerverhalten im Web. (Banking ,Shopping ,Newsgroups...)**
- **Email**
- **eigenes Wissen über Ihr System (Informationsstand)**

Fazit:

Die Gefahr ist allgegenwärtig. Allerdings sind lange nicht alle Angriffe mit einem tatsächlichen Schaden verbunden. Doch sollte Jeder an seinen Schutz denken und nicht darauf hoffen nicht betroffen zu sein. Es ist nur eine Frage der Zeit, bis man Ziel eines Angriffs wird.

Spyware!

Mit der so genannten Spyware bzw. Adware erstellen Softwareunternehmen heimlich ohne Wissen des Anwenders ein Benutzerprofil und senden dieses mit den persönlichen Daten über das Internet an den Hersteller der installierten Software. Die Spyware wird eingesetzt damit die Marketingstrategen in den Softwareunternehmen wissen wie effektiv ihre Werbung ist und möchten dafür natürlich soviel über den Anwender erfahren wie nur möglich.

Virenschutz, Antivirus

Hat der Softwarehersteller die Benutzerinformationen erhalten leitet es diese an ein Werbeunternehmen weiter, wertet die Informationen und belästigt den Anwender anschließend gezielt mit Werbemails.

Besonders stark wird Spyware auch bei durch Werbung finanzierte Freeware verwendet und wird die in der Freeware enthaltene Spywarekomponente durch ein Programm wie Ad-Aware entfernt kann es vorkommen dass sie nicht mehr ohne Probleme läuft.

Die folgenden Informationen sammelt die Spyware:

Aufgerufene Webseite durch den Anwender.

Anwender

Wie lange und zu welcher Zeit der Nutzer im Netz war

Wie lange der Nutzer auf der Webseite war

Suchwörter welche bei der Suchmaschine eingegeben wurden

Welche Software sich auf dem Rechner des Nutzers befindet

Obwohl die Spyware gewisse Gemeinsamkeiten mit Trojanern haben, existieren einige Unterschiede:

Trojaner spionieren persönliche Anwenderdaten wie zum Beispiel Passwörter, Kreditkartennummern usw. heimlich aus während Spyware nur für das Marketing wichtige Benutzerprofile generiert Trojaner schleusen sich heimlich in das System des Anwenders ein während Softwarehersteller den Anwender während der Installation darauf hinweisen, dass ihre Software gewisse Funktionen für die Datenerfassung enthält aber leider sind solche Hinweise nicht sofort erkennbar und meist schlecht formuliert, auch wird sich kein Nutzer bei einer Softwareinstallation die seitenlange Lizenzbedingungen komplett durchlesen.

Informiert eine Spyware den Anwender nicht über ihre Spionagefunktionen, so kann man diese Software auch einen Trojaner nennen.

Auf der Webseite www.tom-cat.com/spybase/index.html gibt es eine Liste in der mehr als 850 Programme aufgelistet sind, welche eindeutig als Spyware bezeichnet werden können.

Fazit:

Sie werden sich wundern in wie vielen und vor allem auch welchen Programmen überall mit Spyware gearbeitet wird. In den USA gibt es diese Diskussion allerdings überhaupt nicht, ob nun zur Datenerfassung ein Spyprogramm wie das von z.B. Gator verwendet werden soll oder nicht.